Issue Number : 5-5-2010-040770517

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : Application Number		20-2004-0009258
출원년월일 : Filing Date		2004년 04월 02일 APR 02, 2004
출원인 : Applicant(s)		이효승 LEE, HYO SEUNG

2010년 07월 26일

특허청

COMMISSIONER

◆ This certificate was issued by Korean Intellectual Property Office. Please confirm any forgery or alteration of the contents by an issue number or a barcode of the document below through the KIPOnet- Online Issue of the Certificates' menu of Korean Intellectual Property Office homepage (www.kipo.go.kr). But please notice that the confirmation by the issue number is available only for 90 days.

출원번호: 20-2004-0009258

【서지사항】

【서류명】 명세서 등 보정서

【수신처】 특허청장

【제출일자】 2004.10.06

【제출인】

【성명】 이효승

【출원인코드】 4-2003-002169-4

【사건과의 관계】 출원인

【대리인】

【성명】 김성기

【대리인코드】 9-1998-000017-6

【포괄위임등록번호】 2003-003428-3

【사건의 표시】

【출원번호】 20-2004-0009258

【출원일자】 2004.04.02

【고안의 명칭】 난수교환 및 연산을 이용한 제품 복제 방지 장치

【제출원인】

【발송번호】 9-5-2004-0371659-45

【발송일자】 2004.09.06

【보정할 서류】 명세서등

【보완할 사항】

【보정대상항목】 별지와 같음

출원번호: 20-2004-0009258

【보정방법】 별지와 같음

【보정내용】 별지와 같음

【취지】 실용신안법시행규칙 제8조의 규정에 의하여 위와 같이 제출합니다.

대리인 김성기 (인)

【수수료】

【보정료】 13,000 원

【추가1년분등록료】 0 원

【기타 수수료】 0 원

【합계】 13,000 원

【첨부서류】 1.보정내용을 증명하는 서류_1통

【보정서】

【보정대상항목】 요약

【보정방법】 정정

【보정내용】

【요약】

본 고안은 개발자와 양산자가 상이한 경우 개발자가 특정반도체를 전기전자제품 등에 내장하여 전기전자제품의 동작을 제어함으로써 제품양산물량을 통제하기 위한 복제방지장치에 관한 것이다. 일반적으로 제품에 대한 복제방지장치 내장은 개발비 및 단가가 비싸므로 양산 단가 상승을 초래하는데, 본 고안의 복제방지장치는 이러한 개발비를 절감하고 단가상승을 최소화 할 수 있도록 함과 아울러, 현재 문제가 심각한 저가 복제품의 무제한 생산으로 인한 영업 손실을 근본적으로 제거할 수 있다. 본 고안은 알고리즘 공유에 의해 생성된 난수 교환방식으로써 제품 동작과정에서 복제방지장치에 임의의 난수를 입력하면 이 난수에 대해 임의의 연산알고리즘에 의한 응답값을 생성한다. 생성된 응답값을 제품의 CPU에 의한 알고리즘 연산 계산값과 비교하여 일치 여부에 따라 본 고안의 복제방지장치의 존재 유무를 판정할 수 있다.

【보정대상항목】 색인어

【보정방법】 정정

【보정내용】

【색인어】

복제방지, 암호화, 난수

【보정대상항목】 식별번호 1

【보정방법】 정정

【보정내용】

[0001] 도 1은 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치의 동작 순서도.

【보정대상항목】 식별번호 2

【보정방법】 정정

【보정내용】

[0002] 도 2는 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치 구성도.

【보정대상항목】 식별번호 3

【보정방법】 정정

【보정내용】

[0003] 도 3은 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치의 칩셋 상세도.

【보정대상항목】 식별번호 5

【보정방법】 정정

【보정내용】

[0005] 21 : 롬테이블 22 : 인터페이스

【보정대상항목】 식별번호 6

【보정방법】 정정

【보정내용】

[0006] 23 : 연산장치 24 : 레지스터

【보정대상항목】 식별번호 7

【보정방법】 정정

【보정내용】

[0007] 27 : 외부제어장치

【보정대상항목】 식별번호 8

【보정방법】 삭제

【보정대상항목】 식별번호 9

【보정방법】 정정

【보정내용】

[0009] 본 고안은 난수교환 및 연산을 이용한 제품복제방지장치에 관한 것이다.

【보정대상항목】 식별번호 10

【보정방법】 정정

【보정내용】

[0010] 종래의 양산체제에서는 개발자와 양산자가 별개의 법인 또는 개인인 경우 개발자가 양산자에게 제품동작방법, 제조방식, 프로그램, PCB 규격, 소자 구동방식 등을 모두 알려주어 제품을 양산하게 하였다.

【보정대상항목】 식별번호 11

【보정방법】 정정

【보정내용】

[0011] 이 경우 개발자는 양산자가 계약에 정해진대로 로열티를 지급하지 않거나 정해진 양산수량을 초과할 경우 법적으로 제소하는 방법 이외에는 마땅한 대책이 없었다. 특히 양산자가 소규모 영세업자 혹은 중국 등 해외인인 경우 국내법의 적용이 쉽지 않을 뿐만 아니라, 정보 유출로 인해 제3자가 동일한 제품을 양산할 경우 적절하게 제재할 수 있는 방법이 제한될 수밖에 없고, 설령 법적인 제재를 가한다고 하더라도 그 비용이 무시하지 못할 수준이다.

이에 따른 해결책으로 종래에는 개발자가 자신이 개발한 제품동작 프로그램이 내장된 마이컴을 직접 공급하기도 하였으나, 이 경우에도 마이컴 단가 및 재고비용증가, 적기공급이 어렵다는 문제점이 수반되었다.

【보정대상항목】 식별번호 12

【보정방법】 정정

【보정내용】

[0012] 본 고안은 상기와 같은 종래의 문제점을 감안하여 이루어진 것으로써 본 고안의 목적은 난수교환 및 연산을 이용하여 전기전자제품내에 복제방지용 칩셋의 내장여부를 판단하고, 그 판단결과에 따라 제품의 동작이 이루어지도록 한 제품복제 방지장치를 제공하는데 있다.

【보정대상항목】 식별번호 13

【보정방법】 정정

【보정내용】

[0013] 상기 목적을 달성하기 위한 본 고안의 난수교환 및 연산을 이용한 제품복제방지장치는, 중앙연산처리장치; 상기 중앙연산처리장치로부터 난수 데이터를 입력받는 인터페이스; 상기 인터페이스로부터의 난수 데이터를 저장하고, 암호화를 위해 사용하는 내부의 상수값을 미리 저장하는 롬테이블; 상기 인터페이스로부터 출력되는 난수 데이터를 랜덤하게 입력받아 상기 롬테이블의 내부의 상수값과 연산하는 연산장치; 상기 연산장치에 의해 연산된 데이터를 저장하는 레지스터; 및 상기 연산장치에 의해 연산된 데이터를 인터페이스로 출력하여 중앙연산처리장치에 미리 저장된 데이터와의 일치여부를 판단하여 제품의 동작여부를 결정토록 하는 출력장치로 구성된 것을 특징으로 한다.

【보정대상항목】 식별번호 14

【보정방법】 정정

【보정내용】

[0014] 본 고안의 상기 중앙연산처리장치는 현재 사용중인 알고리즘의 노출시 다른 알고리즘을 선정하여 인터페이스 가능하도록 복수개의 알고리즘을 저장한 것을 특징으로 한다.

본 고안의 상기 중앙연산처리장치는 암호화 동작 변경시 전체 마스크를 변경하지 않고도 동작변경이 가능토록 암호화를 위해 사용하는 내부의 상수값을 롬테이블로 형성한 것을 특징으로 한다.

【보정대상항목】 식별번호 15

【보정방법】 정정

【보정내용】

[0015] 이하, 본 고안의 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

【보정대상항목】 식별번호 16

【보정방법】 정정

【보정내용】

[0016] 도 1은 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치의 동작 순서도, 도 2는 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치 구성도, 도 3은 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지 칩셋 상세도이다.

【보정대상항목】 식별번호 17

【보정방법】 정정

【보정내용】

[0017] 도 3에 도시한 바와 같이 본 고안의 제품복제방지장치(1)는 중앙연산처리장치(1)와, 전기전자제품인 외부제어장치(27)로부터 제품복제여부를 판단하기 위한 난수 데이터를 입력받는 인터페이스(22)와, 상기 인터페이스(22)로부터의 난수 데이터를 저장하고, 암호화를 위해 사용하는 내부의 상수값이 저장된 롬테이블(21)과, 상기 인터페이스(22)로부터 랜덤하게 출력되는 난수 데이터와 상기 롬테이블(21)에 저장된 상수값을 연산하는 연산장치(23)와, 상기 연산장치(23)에 의해 연산된 데이터를 저장하는 레지스터(24)와, 상기 연산장치(23)에 의해 연산되어 레지스터(24)에 저장된 데이터를 인터페이스(22)로 출력하여 외부제어장치(27)에 미리 저장된 데이터와의 일치여부를 판단하여 제품의 동작여부를 결정토록 하는 출력장치(24)로 구성된다.

【보정대상항목】 식별번호 18

【보정방법】 정정

【보정내용】

[0018] 이와 같은 구성을 갖는 본 고안은 외부제어장치(27)로부터 입력된 난수 데이터가 인터페이스(22)를 통해 롬테이블(21)에 저장되는 가운데 연산장치(23)에서는 상기 난수 데이터를 랜덤하게 입력받아 미리 롬테이블(21)에 저장된 상수값과 연산한 후, 연산 데이터를 레지스터(24)에 임시저장하였다가 인터페이스(22)를 통해 외부

제어장치(27)로 출력하여 외부제어장치(27)에 미리 저장된 데이터와의 일치여부에 따라 제품동작이 가능토록 한다.

【보정대상항목】 식별번호 19

【보정방법】 정정

【보정내용】

[0019] 이때, 본 고안의 복제방지장치는 롬테이블(21) 변경 혹은 연산장치(23)의 연산 로직에 관련된 마스크 데이터만 변경하는 방식으로 전혀 다른 난수교환 칩셋으로 구현될 수 있다. 따라서 소량 다품종의 상이한 암호화 칩셋을 수요로 할 경우 저렴한 비용에 의해서 암호화 동작이 상이한 제품군을 출시할 수 있다.

【보정대상항목】 식별번호 20

【보정방법】 정정

【보정내용】

[0020] 도 1에 도시한 바와 같이 전기전자제품의 외부제어장치(27)는 본 고안의 암호화한 반도체인 복제방지장치 칩셋과 난수 데이터를 인터페이스한다.

【보정대상항목】 식별번호 21

【보정방법】 정정

【보정내용】

[0021] 본 고안의 실시예인 셋톱 박스를 예로 들면 셋톱에 전원이 인가되면 부팅을 하고,

부팅 중에 시계를 읽어서 현시점의 시간을 디지털화하여 이 값을 알고리즘 라이센스 허용 암호화 반도체(난수교환용 칩셋)에 입력한다.

【보정대상항목】 식별번호 22

【보정방법】 정정

【보정내용】

[0022] 난수교환용 칩셋은 상기 데이터를 입력받고 미리 정해진 내부의 상수를 이용하여 예정된 알고리즘 연산방법에 따라 연산된 값을 레지스터(24)에 저장한다.

이때 알고리즘 연산방법은 예를 들면 가감승제, XOR, AND, NAND, NOR 등 입출력간의 데이터 상관성을 찾기 어려운 암호화 방법을 사용하며, 외부제어장치(27)는 난수교환용 칩셋의 알고리즘에 따라 연산한다.

외부제어장치(27)는 자체 연산에 의해 출력된 디지털 변환 시계값을 미리 정해진 상수값과 연산방법에 의해 연산한다(3). 외부제어장치(27)는 난수교환 데이터를 읽어 상기 연산결과값과 비교한다(5)(6). 만일 자체 연산결과값과 읽어낸 데이터가 동일한 경우 다음 과정을 진행하고 동일하지 않은 경우 동작을 멈춘다.

따라서 셋톱 박스의 부팅시 세트동작을 위해서는 난수교환용 칩셋이 반드시 필요하다. 따라서 난수교환용 칩셋이 없다면 동작이 불가능하므로 양산자는 개발자로부터 공급받은 난수교환용 칩셋의 수량만큼만 제품을 생산할 수 있다.

도 2는 난수교환 복제방지 시스템 구성도이다.

무작위로 얻어진 난수데이터 예를 들면 시계 디지털값(16)은 난수교환용 칩셋에서

의 연산출력(18)과 외부제어장치(27)에서의 미리 정해진 연산값(17)을 비교한다(19). 비교결과, 값이 동일한 경우 세트는 라이센스 허용이라 판정하고, 값이 다른 경우 몇 번 더 시도하거나 이상발생시 동작을 멈추도록 한다.

【보정대상항목】 식별번호 23

【보정방법】 정정

【보정내용】

[0023] 상술한 바와 같이 본 고안에 따른 난수교환 및 연산을 이용한 제품복제방지장치에 의하면 다음과 같은 뛰어난 효과가 있다.

【보정대상항목】 식별번호 24

【보정방법】 정정

【보정내용】

[0024] 첫째, 본 고안에 따른 복제방지용 칩셋이 내장되지 않은 제품은 동작이 불가능하기 때문에 개발자는 제품양산수량을 적절하게 조절할 수 있다.

【보정대상항목】 식별번호 25

【보정방법】 정정

【보정내용】

[0025] 예를 들면 한국에서 선진 셋톱박스 개발기술을 가진 개발자가 중국의 양산자에 양산 실시권을 부여하고 이 제품의 양산 허가에 대한 개당 로얄티를 징수할 경우, 현

재의 양산체재에서는 양산자는 불법적으로 개발자의 허락보다 많은 수량을 양산하여 공급할 수 있으며 이에 대한 개발자의 직접적인 통제방법은 전무하다. 그러나 예를 들어 개발자가 셋톱박스를 개발하고 이 제품의 동작에 필수적인 반도체를 공급할 경우 특정 반도체의 물량 통제를 통하여 양산자의 양산허가 개수를 조절할 수 있다. 이때 이 특정 반도체는 개발비나 단가가 매우 저렴하여야만 수월하게 이용할 수 있다.

【보정대상항목】 식별번호 26

【보정방법】 정정

【보정내용】

[0026] 둘째, 반도체 개발시 개발비를 절감할 수 있다. 암호화 반도체 공급의 특성상 한 제품군에는 타사에 공급되는 반도체를 제공하는 것을 선호하지 않는다. 본 고안에서는 반도체 마스크 데이터를 변경할 경우 상수값 알고리즘 로직 등을 롬테이블에 데이터화하여 조정할 수 있도록 하여 최소의 공정비용으로도 별개의 반도체를 생산할 수 있도록 함으로서 소량 다품종 생산이 가능하도록 하였다.

셋째, 복수개의 알고리즘과 상수값을 반도체에 내장하여 동작시킴으로서 알고리즘이 불의의 사고로 공개될 경우에도 개발자는 알고리즘 방식과 상수값 선정을 바꿀 수 있도록 하여 암호화 반도체로서의 연속적인 사용이 가능토록 하였다.

즉, 복수개의 암호화 알고리즘을 내장하여 개발자는 이들 중 한 개를 선택할 수 있게 함으로서 개발자에 의한 현재 사용 알고리즘의 정보오픈이나 알고리즘의 연구에

의해 유사 반도체를 제조할 경우 즉시 이후의 양산 세트에서는 알고리즘 선정과 변경이 가능하도록 하였다. 또한 반도체에서 암호화를 위하여 사용하는 내부의 상수값을 롬테이블로 형성함으로서 반도체 암호화 동작 변경시 전체 마스크를 변경하지 않고도 저렴한 비용으로 동작을 변경할 수 있게 하였다.

【보정대상항목】 청구항 1

【보정방법】 정정

【보정내용】

【청구항 1】

중앙연산처리장치(1);

전기전자제품인 외부제어장치(27)로부터 제품복제여부를 판단하기 위한 난수데이터를 입력받는 인터페이스(22);

상기 인터페이스(22)로부터의 난수 데이터를 저장하고, 암호화를 위해 사용하는 내부의 상수값이 저장된 롬테이블(21);

상기 인터페이스(22)로부터 랜덤하게 출력되는 난수 데이터와 상기 롬테이블(21)에 저장된 상수값을 연산하는 연산장치(23);

상기 연산장치(23)의 연산 데이터를 저장하는 레지스터(24); 및

상기 연산장치(23)에 의해 연산되어 레지스터(24)에 저장된 연산 데이터를 인터페이스(22)로 출력하여 외부제어장치(27)에 미리 저장된 데이터와의 일치여부에 따라 제품의 동작여부를 결정토록 하는 출력장치(24)로 구성된 것을 특징으로 하는 난수

출원번호: 20-2004-0009258
교환 및 연산을 이용한 제품복제방지장치.

【보정대상항목】 청구항 2

【보정방법】 정정

【보정내용】

【청구항 2】

제1항에 있어서, 상기 중앙연산처리장치(1)는 현재 사용중인 알고리즘의 노출시 다른 알고리즘을 선정하여 인터페이스를 가능하게 하도록 복수개의 알고리즘을 저장한 것을 특징으로 하는 난수교환 및 연산을 이용한 제품복제방지장치.

【보정대상항목】 청구항 3

【보정방법】 정정

【보정내용】

【청구항 3】

제1항에 있어서, 상기 중앙연산처리장치(1)는 암호화 동작 변경시 전체 마스크를 변경하지 않고도 동작변경이 가능토록 암호화를 위해 사용하는 내부의 상수값을 롬 테이블로 형성한 것을 특징으로 하는 난수교환 및 연산을 이용한 제품복제방지장치.

출원번호: 20-2004-0009258

【서지사항】

【서류명】 명세서 등 보정서

【수신처】 특허청장

【제출일자】 2004.07.16

【제출인】

【성명】 이효승

【출원인코드】 4-2003-002169-4

【사건과의 관계】 출원인

【사건의 표시】

【출원번호】 20-2004-0009258

【출원일자】 2004.04.02

【고안의 명칭】 난수교환 및 연산을 이용한 제품 복제 방지 장치

【제출원인】

【발송번호】 9-5-2004-0239016-45

【발송일자】 2004.07.16

【보정할 서류】 명세서 등

【보완할 사항】

【보정대상항목】 별지와 같음

【보정방법】 별지와 같음

【보정내용】 별지와 같음

출원번호: 20-2004-0009258

【취지】 실용신안법시행규칙 제8조의 규정에 의하여 위와 같이 제출합니다.

제출인 이효승 (인)

【수수료】

【보정료】 3,000 원

【추가1년분등록료】 0 원

【기타 수수료】 0 원

【합계】 3,000 원

【감면사유】 개인(70%감면)

【감면후 수수료】 3,000 원

【첨부서류】 1.보정내용을 증명하는 서류_1통

【보정서】

【보정대상항목】 식별번호 19

【보정방법】 정정

【보정내용】

[0019] 그림 2 는 난수교환 복제방지 시스템 구성도이다.

【보정대상항목】 식별번호 20

【보정방법】 정정

【보정내용】

[0020] 무작위로 얻어진 난수데이터 예를 들면 시계 디지털 값은 (16), 난수교환 칩셋에서 연산 출력과 CPU 에서의 미리 정해진 연산에 (17) 따른 두 값을 비교한다 (19). 이 결과가 같은 경우 세트는 라이센스 허용이라 판정하고, 두 결과 값이 다른 경우 몇 번 더 시도하거나 하여 이상발생시 동작을 멈추도록 한다. 이를 위한 암호화 반도체 장치의 구성시 장치내부의 연산방법은 27 의 외부 신호에 따른 입력 신호의 선택에 따라 변경이 가능하다.

【보정대상항목】 식별번호 21

【보정방법】 정정

【보정내용】

[0021] 그림 3 은 난수교환 칩셋 내부 구성도 이다. 난수교환 칩셋 외부로부터 입력된 데

이터는 (27) 롬테이블 값을 선정(21) 하고 이 출력값과 랜덤입력 값을(26) 선택하여 연산한후(23) 이 결과값을 내부레지스터(24)에 저장한다. 상기장치에서 그림 3의 27 은 암호화 반도체 외부기기의 입출력 신호장치이며 22 는 암호화할 데이터의 입력및 암호화된 데이터의 출력데이터의 외부기기와 교환장치이다. 암호화시에 연산과정및 연산의 복잡성 증가를 위한 롬테이블은 21 에 사용하였다. 상기 롬테이블에 저장된 임의의 상수를 22 의 입력신호인테페이스 장치로부터 선택하여 상기 출력신호를 23 의 임호화 연산장치와 임의의 연산을 수행하여 24 의 출력 버퍼장치에 저장한다. 상기 24 의 출력 데이터를 외부기기 27 의 출력요정에 따라 출력할 수 있도록 하였다.

【보정대상항목】 식별번호 22

【보정방법】 정정

【보정내용】

[0022] 이때 난수교환 칩셋은 21 번 항목의 롬테이블 변경이나 23 번 연산항복의 연산 로직에 관련된 마스크 데이터만 변경하여 전혀 다른 난수교환 칩셋으로 구현될 수 있다. 이는 소량 다품종의 상이한 암호화 칩셋을 수요로 할 경우 저렴한 비용에 의해서 암호화 동작이 상이한 제품군을 출시 할 수 있다. 상기 21 의 롬테이블 장치나 23 의 연산장치 혹은 22 의 인테페이스 장치를 외부신호장치 27 의 신호 선택에 따라 선택적으로 연산혹은 변경이 가능하도록 한 암호화 반도체장치의 구성이다.

【보정대상항목】 청구항 1

【보정방법】 정정

【보정내용】

【청구항 1】

암호화를 위한 반도체 장치에 있어서 상기장치에 입력된 임의의 값을 반도체 내부의 임의의 상수와 연산하여 결과값을 타장치에서 비교가 가능하도록 출력할 수 있도록 하는 장치.

【보정대상항목】 청구항 2

【보정방법】 정정

【보정내용】

【청구항 2】

암호화를 위한 반도체 장치에 있어서 외부 장치의 선택에 의하여 상기 암화화 장치의 내부의 복수개의 연산과 상수중 임의의 한개를 택일하도록 하는장치

【보정대상항목】 청구항 3

【보정방법】 정정

【보정내용】

【청구항 3】

암호화를 위한 반도체 장치에 있어서 내부의 상수값의 용이한 변경을 위하여 로직 혹은 롬장치를 사용하여 선택이 가능하도록 하는 장치

출원번호: 20-2004-0009258

【서지사항】

【서류명】 실용신안등록출원서

【수신처】 특허청장

【제출일자】 2004.04.02

【국제특허분류】 H01L

【고안의 국문명칭】 난수교환 및 연산을 이용한 제품 복제 방지 장치

【고안의 영문명칭】 The apparatus of copy protection system by use of the exchange random vvariable and the arbitrary operation

【출원인】

【성명】 이효승

【출원인코드】 4-2003-002169-4

【특기사항】 대표자

【지분】 100/100

【고안자】

【성명】 이효승

【출원인코드】 4-2003-002169-4

【특허(등록)증 수령방법】 우편수령

【취지】 실용신안법 제9조의 규정에 의하여 위와 같이 제출합니다.

출원인 이효승 (인)

【수수료】

【기본출원료】 0 면 17,000 원

출원번호: 20-2004-0009258

【가산출원료】	12 면 0 원
【최초1년분등록료】	3 항 35,000 원
【우선권주장료】	0 건 0 원
【합계】	52,000 원
【감면사유】	개인(70%감면)
【감면후 수수료】	15,600 원
【첨부서류】	1.요약서 · 명세서(도면)_1통

출원번호: 20-2004-0009258

【요약서】

【요약】

본 고안은 복제 방지 장치에 관한 것으로서, 개발 회사와 양산회사가 상이한 경우 개발회사가 특정반도체를 사용하여 양산물량을 통제 하는 것을 목적으로 하는 반도체 장치에 관한 것이다. 외주 양산 업체를 이용하여 제품을 생산할 경우, 당 반도체를 내장 생산 하여 당 반도체가 없을 경우 동작이 불가능하게 하거나 본 칩셋의 내장여부를 손쉽게 확인 하도록 하는 장치에 관한 것이다. 일반적으로 반도체 탑재는 개발비가 비싸고 단가도 적지 않으므로 양산 단가가 상승하게 되는데, 본 고안의 방법 또는 장치는 이러한 개발비를 상승을 절감하고 단가상승을 최소화 할 수 있도록 하였다. 이로서 저렴한 비용의 당 반도체 탑재로 현재 문제가 심각한 저가 무제한 복제품 생산에 의한 영업 손실을 근본적으로 제거할 수 있게 한 장치 및 방법에 관한 것이다.

당 고안의 요체는 알고리듬 공유에 의하여 생성된 난수 교환을 사용한다. 당 방식은 시스템이 임의의 동작과정에서 반도체에 임의의 난수를 입력하고 이 난수를 반도체 내부에서 임의의 연산 알고리듬에 의한 응답 값을 생성하게 하는 장치 및 방법이다. 생성된 결과를 반도체로부터 읽어볼 수 있도록 하여 CPU 내부의 미리 약속된 알고리듬 연산 계산값과 비교하여 반도체 당 칩셋의 존재 유무를 판정할 수 있게 하였다.

【대표도】

도 1

【색인어】

Random Variable, operation, Consumer, Electronics, Copy, Password, settop box, TV, VCR, Semiconductor

【명세서】

【고안의 명칭】

난수교환 및 연산을 이용한 제품 복제 방지 장치 { The apparatus of copy protection system by use of the exchange random vvariable and the arbitrary operation }

【도면의 간단한 설명】

[0001] 도 1 은 난수교환 및 연산을 이용한 제품 복제 방지 장치 시스템 동작 순서도

[0002] 도 2 은 난수교환 및 연산을 이용한 제품 복제 방지 장치 시스템 구성도

[0003] 도 3 은 난수교환 및 연산을 이용한 제품 복제 방지 장치 칩셋 세부구성도

[0004] * 도면의 주요부분에 대한 부호의 설명 *

[0005] 1. ----- 난수교환 및 연산 칩셋

[0006] 11. ----- 세트 메인 제어장치

[0007] 21. ----- ROM 테이블

[0008] 22. 외부 인터페이스 장치

【고안의 상세한 설명】

【고안의 목적】

【고안이 속하는 기술분야 및 그 분야의 종래기술】

[0009] 종래의 양산 장치에서 개발회사와(; 이하 개발자) 양산회사가(;이하 양산자) 별개의 법인 또는 개인인 경우 양산을 위해서는 개발자가 양산자 에게 제품동작방법, 제조방식, 프로그램, PCB 규격, 소자 구동방식 등을 모두 송부 하여 양산하게 하였다. 이 경우 개발자는 양산자가 계약대로 로열티를 지급하거나 양산수량을 초과하여 양산할 경우 법적인 제소등 이외에는 제제가 불가능 하였다. 양산자가 소규모이든가, 양산자가 중국등 국외인 경우 법등의 적용이 쉽지 않으며 또한 정보의 유출에 의하여 타사에서 개발제품과 동일한 제품을 양산할 경우에 제제할 수 있는 방법이 제한되었고 이에 따른 법적 제제 등에 따른 제반비용이 증가하였다. 종래의 장치에서는 개발자가 자신이 개발한 제품동작 프로그램이 탑재된 마이컴을 직접 공급함으로서 이러한 문제를 해결하려고 하였으나 마이컴 재고비용증가, 마이컴 마스크 단가 및 적기공급의 애로사항이 발생하였다.

[0010] 당 발병에서는 개발자에게 저렴한 비용에 양산 복자방지 전용 반도체를 탑재할 수 있도록 하여 본 고안의 반도체가 없을 경우 전자제품의 작동을 멈추는 등의 작동을 하도록 프로그램을 할 수 있도록 제품 복제방지 반도체를 설계 하였다.

[0011] 이에 따라 법적인 제소 등의 방법을 사용하지 않고도 저렴한 당 반도체 의 장착에 의하여 개발자의 의도대로 직접 양산자의 양산물량을 컨트롤 할 수 있도록 하게 하였다.

【고안이 이루고자 하는 기술적 과제】

[0012] 본 고안은 복제 방지를 위한 암호화 반도체의 간단한 구성과 이 칩셋의 구현 방법 및 장치에 관한 것이다. 양산을 실시할 경우 미미한 추가 비용 부담에 의해 무단 복제품을 원 소유자의 허가 없이 양산할 수 없도록 한 장치이다. 당 반도체가 없을 경우 세트는 동작하지 않도록 하여 개발자는 당 반도체를 양산을 허가한 수량만큼 만 공급하는 것으로 양산 수량을 제어할 수 있다. 예를 들면 한국에서 선진 Set-Top Box 개발기술을 가진 개발자가 중국의 양산자에 양산 실시권 을 부여하고 이 제품의 양산 허가에 대한 개당 로얄티를 징수할 경우, 현재의 방법에서는 양산자는 불법적으로 개발자의 허락보다 많은 수량을 양산하여 공급할 수 있으며 이에 대한 개발자의 직접적인 통제방법은 전무한다. 그러나 예를 들어 개발자가 Set-Top Box 를 개발하고 이 제품의 동작에 필수적인 반도체를 공급할 경우 특적 반도체의 물량 통제를 통하여 양산자의 양산허가 개수를 조정할 수 있다. 이때 이 특정 반도체는 개발비나 단가가 매우 저렴 하여야만 수월하게 이용할 수 있다. 본 고안은 이 동작에 필수적인 특정 반도체의 동작 방식을 설명하고, 특정반도체의 저렴한 개발비 구현 및 단가 부담을 최소화 하는 방법 과 장치에 관한 것이다.

[0013] 본 고안에서는 간단한 제어장치간의 인터페이스에 의하여 본 반도체의 존재여부를 판독할 수 있게 하였다. 만일 본 반도체가 없거나 부적절한 출력을 제어장치에 출력 할 경우 제어장치는 시스템 동작을 중단시키게 한다면 불법복제품은 당 반도체가 없을 경우 양산이 불가능할 것이다.

[0014] 또한 복수개의 암호화 알고리듬을 탑재하여 개발자는 이들 중 한 개를 선택할 수 있게 함으로서 개발자에 의한 현재 사용 알고리듬의 정보오픈이나 알고리듬의 연구에 의해 유사 반도체를 제조 할 경우 즉시 이후의 양산 세트에서는 알고리듬 선정과 변경이 가능하도록 하였다. 또한 반도체에서 암호화를 위하여 사용하는 내부의 상수값을 롬테이블로 형성함으로서 반도체 암호화 동작 변경 시 전체 마스크를 변경하지 않고도 저렴한 비용으로 동작을 변경할 수 있게 하였다.

【고안의 구성】

[0015] 당 고안의 구성은 외부전기전자 제어장치 (그림1 의 2) 와 난수교환 칩셋 (그림1의 1) 로 구현된다. 난수교환 칩셋 내부 구조는 그림 3 에서 외부 제어장치와 인터페이스하는 장치 (22) 와 위 인터페이스 출력을 롬테이블 (21) 과 연산장치 (23) 의 결선에 연결된다. 연산장치 (23) 의 출력은 결과값 출력 장치 (24) 에 의해 외부 인터페이스 (22) 와 연결되며 이 출력은 외부 CPU 와 연결된다.

[0016] 그림 1 은 난수교환 복제방지시스템 동작순서도이다.

[0017] 그림 1 의 1 은 전기 전자 제품의 제어장치이다. 이 제어장치는 2 의 암호화 반도체와 인터페이스 한다. 본 고안의 여하한 실시예인 셋탑 박스를 예를 들면 셋탑에 전원이 인가되면 부팅을 한다. 부팅 중에 시계를 읽어서 현시점의 시간을 디지털화하고 이 값을 알고리듬 라이센스 허용 암호화 반도체 (; 이하 난수교환 칩셋) 에

입력한다. 난수교환 칩셋은 상기데이터를 입력받아 미리 정해진 내부의 상수를 이용하여 예정된 알고리듬 연산방법에 따라 결과값을 레지스터에 저장한다. 이때 알고리듬 연산방법은 임의의 전산 예를 들면 가감승제, XOR, AND, NAND, NOR 등 입출력간의 데이터 상관성을 찾기 어려운 암호화 방법을 사용하며, 제어장치는 난수교환 칩셋의 알고리듬에 따라 연산한다.

[0018] (4번). 제어장치 (이하 CPU) 는 자체 연산에 의하여 출력된 디지털 변환 시계 값을 제어장치의 미리 정해진 상수 값과 연산 방법에 의하여 연산한다 (3 번). CPU 는 난수교환 의 데이터를 읽어서 자신의 연산결과와 비교 한다 (5, 6). 만일 자체 연산한 결과와 읽어낸 결과가 동일한 경우 다음 과정을 진행하고 동일하지 않은 경우 동작을 멈춘다. 따라서 셋탑 박스의 부팅시 세트동작을 위해서는 난수교환 칩셋이 반드시 필요하다. 따라서 난수교환 칩셋이 없다면 동작이 불가함으로 양산자는 개발자로부터 주어진 난수교환 칩셋의 공급량 만큼만 생산할 수 있다.

[0019] 그림 2 는 난수교환 복제방지 시스템 구성도이다.

[0020] 무작위로 얻어진 난수데이터 예를 들면 시계 디지털 값은 (16), 난수교환 칩셋에서 연산 출력과 CPU 에서의 미리 정해진 연산에 (17) 따른 두 값을 비교한다 (19). 이 결과가 같은 경우 세트는 라이센스 허용이라 판정하고, 두 결과 값이 다른 경우 몇 번 더 시도하거나 하여 이상발생시 동작을 멈추도록 한다.

[0021] 그림 3 은 난수교환 칩셋 내부 구성도 이다. 난수교환 칩셋 외부로부터 입력된 데이터는 (27) 롬테이블 값을 선정(21) 하고 이 출력값과 랜덤입력 값을(26) 선택하여 연산한후(23) 이 결과값을 내부레지스터(24)에 저장한다.

[0022] 이때 난수교환 칩셋은 21 번 항목의 롬테이블 변경이나 23 번 연산항복의 연산 로직에 관련된 마스크 데이터만 변경하여 전혀 다른 난수교환 칩셋으로 구현될 수 있다. 이는 소량 다품종의 상이한 암호화 칩셋을 수요로 할 경우 저렴한 비용에 의해서 암호화 동작이 상이한 제품군을 출시 할 수 있다.

【고안의 효과】

[0023] 당 고안은 난수 입력과 알고리듬 연산에 의한 출력을 이용하여 세트 복사를 방지하도록 하는 반도체장치로서 그 효과는 세 가지이다.

[0024] 첫째는 당 반도체가 탑재되지 않은 세트는 동작이 불가능하기 때문에, 세트 개발업체는 당 반도체의 수량 컨트롤에 의하여 양산수량을 적절하게 조장할 수 있다. 당 반도체가 없을 경우 동작자체가 불가능하기 때문에 개발업체는 당 반도체의 공급수량 여하에 따라 양산허가 및 양산 물량을 적절하게 조정할 수 있다.

[0025] 둘째는 반도체 개발시 개발비를 절감할 수 있도록 하였다. 암호화 반도체 공급의 특성상 한 제품군에는 타사에 공급되는 반도체를 제공할 경우를 선호하지 않는다. 본 고안에서는 반도체 마스크 데이터를 변경할 경우 상수값 알고리듬 로직 등을 롬 데이터화 하여 조정할 수 있도록 하여 최소의 공정비용으로도 별개의 반도체를 생산할 수 있도록 함으로서 소량 다품종 생산이 가능하도록 하였다.

[0026] 셋째 복수개의 알고리듬과 상수 값을 반도체에 탑재하여 동작시킴으로서 알고리듬이 불의의 사고로 공개될 경우에도 개발자는 알고리듬 방식과 상수 값 선정을 바꿀

수 있도록 하여 암호화 반도체로서의 연속적인 사용을 가능 하도록 하였다.

【실용신안등록청구범위】

【청구항 1】

난수교환 혹은 복제 방지용 반도체 부품을 탑재한 장치 및 방법에 있어서, 상기장치에 입력된 신호를 반도체 내부의 임의의 값과 임의의 연산을 한 후 이 결과 값을 상기장치를 제어하는 부분에서 읽거나 보낼 수 있도록 하여 결과값을 비교검토 할 수 있도록 하는 알고리듬에 의한 암호화 장치

【청구항 2】

난수교환 혹은 복제 방지용 반도체 부품을 탑재한 장치 및 방법에 있어서 복수개의 알고리듬을 탑재하여, 현재 사용 중인 알고리듬 또는 필요한 상수의 노출 시에도, 다른 알고리듬 또는 상수를 선정하여 인터페이스를 가능하게 함으로서 노출되지 않은 알고리듬을 사용한 반도체의 계속적인 이용이 가능하도록 한 장치 및 방법

【청구항 3】

난수교환 혹은 복제 방지용 반도체 부품을 탑재한 장치 및 방법에 있어서 상기 장치 내부의 롬 테이블 마스킹 데이터혹은 알고리듬 연산에 관련된 반도체 마스크만 변경하여, 전체적인 반도체 마스크변경 개발비를 사용하지 않고도 상기 장치의 암호화 동작을 변경시키도록 한 방법 및 장치

【도면】

【도 1】

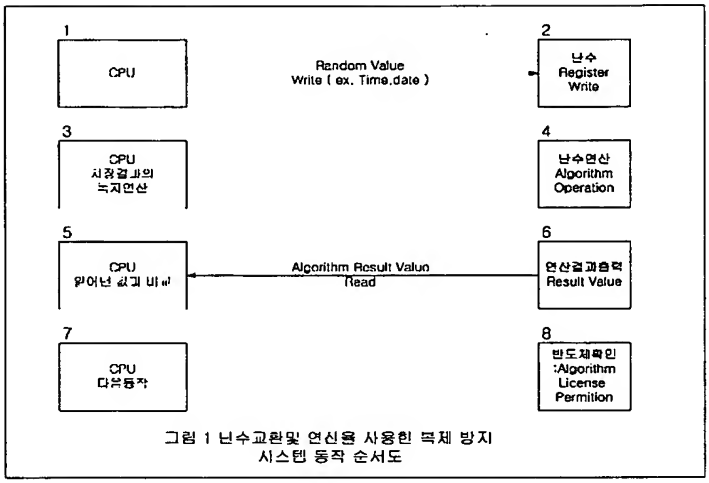

그림 1 난수교환및 연산을 사용한 복제 방지 시스템 동작 순서도

【도 2】

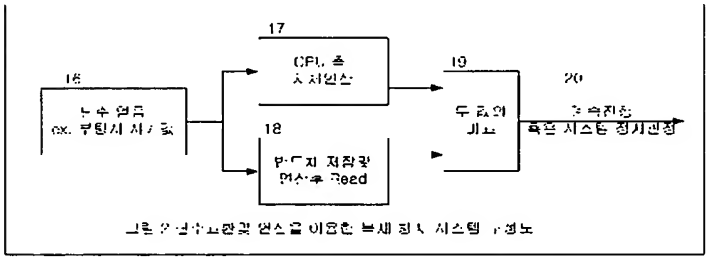

그림 2 난수교환과 연산을 이용한 복제 방지 시스템 구성도

【도 3】